REMARKS

Entry of this amendment, reconsideration, and allowance are respectfully requested. Entry is proper because the amendment incorporates the subject matter of dependent claims 8 and 9 into claim 1 and the subject matter of claims 18 and 19 incorporated into claim 11. No new issues requiring further search are raised, and the amendments simplify the issues for any appeal.

All claims remain stand rejected under 35 U.S.C. §102 for anticipation based on Alsberg. This rejection is respectfully traversed.

Alsberg discloses a protector device as described for enhancing the security of a system which includes user terminals communicating with one or more host computers via a network. A detection means monitors communications between the terminals and the host computers and can detect information transmitted between the computers and terminals and filter it by either blocking it or by editing it before transmitting it. The detection means also includes an audit trail mechanism that performs audit trail recording and analysis. The audit trail mechanism provides details of what happened to any sensitive data that was requested to be transferred. The detection means further includes means for generating an alarm in the event that certain potentially sensitive events occur and means for interrogating events generated and stored in the detection means. Unlike the claims of the instant application, Alsberg is not directed to monitoring a single processor to find any faults that may be present in a particular domain of that processor.

The rejection glosses over several features of claims 1 and 11. The Examiner fails to specifically identify what in Alsberg corresponds to the "plurality of modes" in the computer 18

and what in Alsberg corresponds to the "first domain and second domain" in the computer 18, where the processor modes are different from each other and from the different domains.

In the final action, the Examiner equates communicating or transferring data between a terminal 16 and computer 18 via access node 12, local area network 20, network transceivers, and access node 14 with capturing diagnostic data. The Examiner further equates blocking communication of data between a terminal 16 and computer 18 to suppressing the capture of diagnostic data. With regard to original claims 8, 18 and 9, 19 directed to debug and trace functions that are now incorporated in their respective independent claims, the Examiner equates Alsberg's audit trail analysis to either debugging or tracing.

Assuming for the sake of argument that the audit trail analysis is interpreted as equivalent to debug or trace, a *consistent* application of the terms that the Examiner identifies from Alsberg for the entirety of each claim demonstrates that Alsberg fails to teach all the features of claims 1 and 11. For example, claim 1 requires that the diagnostic data is captured in response to performing the audit trail analysis (equated with performing a debug or trace function). Thus, the claimed diagnostic data is equated by the Examiner to the audit trail data. In col. 6, lines 39-65 of Alsberg, an audit capture command is generated in response to potentially sensitive information being transmitted between a terminal and a computer. In response to this audit capture command, the access node 14 transfers audit information to the command filter module to an audit-trail recording module 66 on the security server 22 via communications media between the access node and security server. The access node also blocks or modifies the transfer of data between the terminal and host computer identified by the command filter.

Recall that in claim 1 capturing of diagnostic data relating to activities of the processor is suppressed. Recall also that the Examiner equated the claimed diagnostic data to Alsberg's audit

trail data. But Alsberg's access node 22 does not block the audit trail data. Nor is there any reason to do so because the audit trail data is sent to the security server 22 and because the audit trail data is required in order to analyze what secure data has been blocked and what has not. Thus, interpreting the diagnostic data as being generated in response to the audit trail analysis equates it to the audit trail data, and the audit trail data is never suppressed or blocked. Although the audit trail data may contain information about the blocking of transfer of sensitive data, this audit trail data is not itself suppressed. Consequently, Alsberg fails to disclose the suppressing of the capture of diagnostic data (not just "communications between computers 18 and terminals 16" as advanced by the Examiner) where diagnostic data is captured in response to performing a debug or trace function.

Another difference is that Alsberg controls security by controlling the transfer of data from a computer to other terminal devices. In contrast, the claims relate to the security of information within a processor and to preventing data leakage between different domains within that processor. As pointed out above, the Examiner fails to show where Alsberg discloses a processor with the claimed plural modes and plural domains. The claimed monitoring logic performs a debug or trace function to monitor the processor. That is not described in Alsberg. Instead, the monitoring function in Alsberg monitors the transfer of information between two physically different and distinct devices. So Alsberg is not concerned with a single processor/computer having different domains or monitoring a single processor/computer itself. The security in Alsberg is focused on the control of data output from the processor/computer and transferred to other devices via a network, which is why the monitoring function monitors the data transfer over the network and not the processor/computer itself. Because Alsberg is not concerned with a processor operable in a plurality of modes and a plurality of domains, Alsberg

also fails to "control said monitoring logic in dependence on said at least one control parameter and the domain in which said processor is operating."

Lacking multiple features recited in the claims, the anticipation rejection is in error and should be withdrawn. The application is in condition for allowance.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100